Lecture 2

Question 1. Prove the contrapositive.

Answer. Recall $A \Rightarrow B$ in terms of logical quantifiers and apply commutativity.

Question 2. State the Peano axioms defining $\mathbb{N}$.

Answer. The natural numbers $\mathbb{N}$ is a set containing the element '1' with an operation '+1' satisfying
(i) $\forall n \in \mathbb{N}$, $n + 1 \neq 1$;
(ii) $\forall m, n \in \mathbb{N}$, if $m \neq n$, then $m + 1 \neq n + 1$;
(iii) for any property $P(n)$, if $P(1)$ is true and $\forall n \in \mathbb{N}$, $P(n) \Rightarrow P(n+1)$, then $P(n)$ is true for all natural numbers.

Question 3. Define the operation '+k' for $k \in \mathbb{N}$ in terms of '+1'.

Answer. For every natural number n, $n + (k + 1) = (n + k) + 1$.
This is defined by induction on $P(k) =$ " '$+k$' is defined"

Lecture 3

Question 4. Show WPI and SPI are equivalent.

Answer. To show WPI implies SPI, apply the former to $Q(n) =$ "$P(m)\ \forall\ m \leq n$". To SPI implies WPI is self-evident.

Question 5. What is the well-ordering principle?

Answer. If $P(n)$ holds for some $n \in \mathbb{N}$, then there is a least $n \in \mathbb{N}$ s.t. $P(n)$ holds.

Question 6. Prove that SPI is equivalent to WOP.

Answer. Consider P(n) false and apply WOP and premises of SPI to obtain contradiction to show WOP implies SPI. To show SPI implies WOP, suppose no n st. $P(n)$ and consider $Q(n) = \neg(P(n))$ with SPI.

Lecture 4

Question 7. Define the highest common factor c of $a, b \in \mathbb{N}$

Answer. (i) $c|a$ and $c|b$
(ii) $d|a$ and $d|b \Rightarrow d|c$.

Question 8. Define the highest common factor c of $a, b \in \mathbb{N}$

Answer. (i) $c|a$ and $c|b$
(ii) $d|a$ and $d|b \Rightarrow d|c$.

Lecture 5

Question 9. State Euclid's algorithm on $a, b \in \mathbb{N}$

Answer. Note: $r_{i+1} < r_i < a$
$a = q_1 b + r_1$
$b = q_2 r_1 + r_2$
$r_1 = q_3 r_2 + r_3$
$r_{n-2} = q_n r_{n-1} + r_n$
$r_{n-1} = q_{n+1} r_n + 0$
Output: r_n

Question 10. Prove Euclid's algorithm returns the hcf of its input.

Answer. Prove properties by induction

Question 11. State Bezouts Theorem

Answer. Let $a, b \in \mathbb{N}$. Then the equation

$$ax + by = c$$

has a solution in the integers iff $(a, b)|c$.

Question 12. Prove Bezouts Theorem with Euclid's algorithm

Answer. Run Euclid's algorithm with input a, b to obtain an output r_n. At step n, we have $r_n = xr_{n-1} + yr_{n-2}$ for some $x, y \in \mathbb{Z}$. Continuing by induction we have $\forall i = 2, \ldots, n-1, r_n = xr_i + yr_{i-1}$ for some $x, y \in \mathbb{Z}$. Thus $r_n = xa + yb$ for some $x, y \in \mathbb{Z}$ from step 1 and 2.

Question 13. Prove $\forall a, b \in \mathbb{N}$, $\exists x, y \in \mathbb{Z}$ s.t. $xa + yb = \text{hcf}(a, b)$ by minimality argument.

Answer. Let h be the least positive linear integer of the form $xa + yb$ for some $x, y \in \mathbb{Z}$.
Use divisibility and minimality to show it satisfies conditions for hcf.

Question 14. Prove if p is a prime and $p|ab$, then $p|a$ or $p|b$.

Answer. Suppose $p \nmid a$ and show $p|b$ using Bezout.

Question 15. (Fundamental theorem of arithmetic) Prove every natural number $n \leq 2$ is expressible as a product of primes, uniquely up to ordering.

Answer. Factorisation can be shown by induction.
For uniqueness, suppose two different factorisations, reorder, divide out with $p|ab$ lemma and use induction.

Lecture 6

Lecture 7

Question 16. Prove inverses are unique modulo n.
Answer. Untangle definitions.

Question 17. Prove a has an inverse modulo n iff $(a, n) = 1$
Answer. Chain of equivalences using Bezout.

Lecture 8

Question 18. State the Chinese Remainder Theorem
Answer. Let m, n be coprime and $a, b \in \mathbb{Z}$. Then there is a unique solution modulo mn to the simultaneous congruences
$equiva \mod m$ and $x \equiv b \mod n$.

Question 19. Prove the Chinese Remainder Theorem
Answer. Use Bezout $(m, n) = 1$ to construct an x which satisfies conditions Show uniqueness by considering new solution y taken $\mod m, n$ and combine algebraically to show it is congruent $\mod mn$.

Question 20. State Fermats Little Theorem
Answer. Let p be prime. Then $a^p = a \mod p \forall a \in \mathbb{Z}$. Equivalently, $a^{p-1} \cong 1 \mod p\ \forall\ a \not\equiv 0 \mod p$

Question 21. Prove Fermats Little Theorem
Answer. If $a \not\equiv 0 \mod p$, then a is a unit $\mod p$. Hence the numbers $a, 2a, \ldots, (p-1)a$ are pairwise incongruent modulo p and $\equiv 0 \mod p$, so they are $1, 2, \ldots, p-1$ in some order. Hence

$$a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \mod p = 1 \cdot 2 \ldots \cdot (p-1)$$

or

$$a^{p-1}(p-1)! \equiv (p-1)! \mod p$$

But we can cancel it to obtain $a^{p-1} \equiv 1 \mod p$.

Question 22. State the Fermat-Euler Theorem
Answer. Let $(a, m) = 1$. Then $a^{\phi(m)} \equiv 1 \mod m$.

Question 23. Prove the Fermat-Euler Theorem
Answer. Consider the set of units modulo m and apply same rearrangement argument as FLT.

Lecture 9

Question 24. Let p be a prime. Then $x^2 \equiv 1 \iff x \equiv +1 \mod p$ or $x \equiv -1 \mod p$.

Answer. Convert $p|ab$ lemma into a modular arithmetic statement and apply.

Question 25. State Wilson's theorem

Answer. Let p be prime. Then $(p-1)! \equiv -1 \mod p$

Question 26. Prove Wilson's theorem

Answer. True for $p = 2$, so assume $p > 2$. Consider pairing up elements and recall ± 1 are the only self-inverse.

Question 27. Let p be an odd prime. Prove that then -1 is a square $\iff p \equiv 1 \mod 4$.

Answer. For $p \equiv 1 \mod 4$,
Apply Wilson's theorem and manipulate to find explicit expression for element which squares to -1. For $p \not\equiv 1 \mod 4$,
Apply FLT to obtain $1 \equiv -1 \mod p$.

Question 28. Outline the RSA Scheme

Answer. I think of two large primes, p, q.
Let $n = pq$ and pick and *encoding exponent* e coprime to $\phi(n) = (p-1)(q-1)$.
I publish the pair (n,e).

To send me a message (ie a sequence of numbers) you chop it into pieces/numbers $M < n$ and send me $M^e \mod n$, computed quickly by repeated squaring.

To decrypt, I work out d st. $ed \equiv 1 \mod \phi(n)$.
Then I compute $(M^e)^d = M^{k\phi(n)+1}$ for some $k \in \mathbb{Z}$
$=M \mod n$ by Fermat-Euler.

Lecture 10

Question 29. Prove (a level style) there is no rational x with $x^2 = 2$.

Answer. Suppose $x^2 = 2$. We may assume $x > 0$ since $(-x)^2 = x^2$. If x is rational, then $x = \frac{a}{b}$ for some $a, b \in \mathbb{N}$. Thus $\frac{a^2}{b^2} = 2$, or $a^2 = 2b^2$. But the exponent of 2 in the prime factorisation is even while the exponent of 2 in $2b^2$ is odd, contradicting the FTA.

Question 30. Prove (constructively) there is no rational x with $x^2 = 2$.

Answer. Suppose $x^2 = 2$ for some $x = \frac{a}{b}$ with $a, b \in \mathbb{N}$. Then for any $c, d \in \mathbb{Z}$ $cx + d$ is of the form $\frac{e}{b}$ for some $e \in \mathbb{Z}$. Thus if $cx + d > 0$, then $cx + d > \frac{1}{b}$.
Thus if $cx + d > 0$, then $cx + d > \frac{1}{b}$.
But $0 < x - 1 < 1$ since $1 < x < 2$.
So if n is sufficiently large,

$$0 < (x-1)^n < \frac{1}{b}$$

But for any $n \in \mathbb{N}$, $(x-1)^n$ is of the form $cx+d$ for some $c, d \in \mathbb{Z}$, since $x^2 = 2$. This is a contradiction.

Question 31. State the least upper bound axiom.

Answer. Given any set S of reals that is non-empty and bounded above, S has a least upper bound.

Lecture 11

Question 32. State the Axioms of Archimedes

Answer. $\mathbb{N}$ is not bounded above in $\mathbb{R}$.
$\exists n in \mathbb{N}$ s.t. $nx > y$ $\forall x, y \in \mathbb{R}$.

Question 33. Prove the Axioms of Archimedes

Answer. Suppose supremum of $\mathbb{N}$ existed and show a greater $n \in \mathbb{N}$ exist.

Question 34. Prove that for all $t > 0$, $\exists n \in \mathbb{N}$ with $\frac{1}{n} < t$.

Answer. Given $t > 0$, there is an $n > \frac{1}{t}$ by Archamedian property, hence $\frac{1}{n} < t$.

Question 35. Prove that there exists $x \in \mathbb{R}$ with $x^2 = 2$.

Answer. Construct a set, and prove supremum satisfies $x^2 = 2$.

Lecture 12

Question 36. What does it mean for the rationals to be dense in $\mathbb{R}$?

Answer. $\forall a < b \in \mathbb{R}$, $\exists c \in \mathbb{Q}$ with $a < c < b$.

Question 37. Prove the rationals are dense in the reals

Answer. We may assume that $a \leq 0$.

By Archimedian property, $\exists n \in \mathbb{N}$ with $\frac{1}{n} < b - a$.
By the Axiom of Archimedes, $\exists N \in \mathbb{N}$ s.t. $N > b$.
Let $T = \{k \in \mathbb{N} : \frac{k}{n} \leq b\}$

then $Nn \in T$, so $T \neq \emptyset$.
By WOP, T has a least element m. Set c = (m-1)/n.
Since $m - 1 \notin T, c < b$.
If $c \leq a$, then $\frac{m}{n} = c + \frac{1}{n} < a + b - a = b$
Which is a contradiction, hence $a < c < b$.

Question 38. When do we say that the sequence $a_1, a_2, a_3, \ldots$ tends to the limit $l \in \mathbb{R}$?
Answer. $\forall \epsilon > 0, \exists N \in \mathbb{N}$ s.t. $n \leq N$, $|a_n - l| < \epsilon$.

Lecture 13

Question 39. Prove that every bounded monotonic sequence converges.
Answer. Show that sequence converges to supremum.

Question 40. Prove that if $a_n \leq d \, \forall n$ and $a_n \to c$ as $n \to \infty$, $c \leq d$.
Answer. Think about this geometrically for intuition, assume for contradiction.

Lecture 14

Question 41. Does every x, $0 \leq x < 1$ have a decimal expansion?
Answer. Construct a sequence of x_k such that you can pick a maximal element to generate the decimal expansion of x.

Question 42. Prove that if a decimal is periodic, then it is rational.
Answer. Find the rational expression for it

Question 43. Prove that if a decimal is rational, then it is periodic.
Answer.

Question 44. Prove e is irrational.
Answer. Suppose $e = \frac{p}{q}$. This would mean $q!e$ is integral.
Consider the infinite expansion ot show that $q!e = N + x$ where $N \in \mathbb{N}$, and $0 < x < 1$, by bounding with geo series. Contradiction.

Lecture 15

Question 45. Prove that, for any polynomial P, $\exists$ constant K such that

$$|P(x) - P(y)| \leq K|x - y| \;\; \forall 0 \leq x, y \leq 1$$

.

Answer. Suppose

$$P(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$$

Consider $P(x) - P(y)$ and factor out $(x - y)$ and bound to find a const.

Question 46. Prove that a non-zero polynomial of degree d has at most d roots.

Answer. Induction on number of roots for polynomial of degree d, rewrite the polynomial as a product of new root and some polynomial $q(x)$ by long division.

Question 47. Prove the number

$$L = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$$

is transcendental.

Answer. Suppose L is the root of a polynomial P.
There exists a K such that $|P(x) - P(y)| \leq K|x - y| \;\; \forall 0 \leq x, y \leq 1$.
do it do it do it do it do it do it do it do it do it do it do it do it do it do it do it do it do it

Lecture 16

Question 48. If A is a set and P is a property of (some) elements of A, how do we write the subset of A comprising of those elements for which $P(x)$ holds?

Answer.

$$x \in A : P(x)$$

Question 49. Write $A \backslash B$ in set notation

Answer.

$$\{x \in A : x \notin B\}$$

Question 50. If $A_1, A_2, A_3, \ldots$ are sets then what is

$$\cap_{n=1}^{\infty} A_n?$$

Answer. $\{x : x \in A_n \text{ for all } n \in \mathbb{N}\}$

Question 51. Prove you cannot form $\{x : P(x)\}$

Answer. Construct $X = \{x : x \text{ is a set and } x \notin x\}$,
and consider whether $X \in X$

Lecture 17

Question 52. Define the binomial coefficient $\binom{n}{k}$

Answer.

$$\binom{n}{k} = \left|\{S \subseteq \{1, 2, \ldots, n\} : |S| = k\}\right|$$

Question 53. State the inclusion-exclusion principle

Answer.

$$|S_1 \cup S_2 \cup \ldots \cup S_n| = \sum_{|A|=1} |S_a| - \sum_{|A|=2} |S_A| + \sum_{|A|=3} |S_A| - \ldots + (-1)^{n+1} \sum_{|A|=n} |S_A|$$

where $S_A = \cap_{i \in A} S_i$ Equivalently,

$$|\bigcap_{i=1}^{n} S_i| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{\substack{A \subseteq \{1,2,\ldots,n\} \\ |A|=k}} |\bigcap_{i \in A} S_i|.$$

Question 54. Prove the inclusion-exclusion principle.

Answer. Suppose $x \in S_i$ k times and prove that it is only counted once via counting.

Lecture 18

Question 55. Formally define a function $f : A \to B$.

Answer. A function from A to B is a subset $f \subseteq A \times B$ such that for all $x \in A$, there is a unique $y \in B$ such that $(x, y) \in f$.

Question 56. When do we say that a function $f : A \to B$ is injective?

Answer. $\forall a, a' \in A$,
$a \neq a' \Rightarrow f(a) \neq f(a')$, or equivalently
$f(a) = f(a') \Rightarrow a = a'$.

Question 57. When do we say that a function $f : A \to B$ is surjective?

Answer. If $\forall b \in B$, $\exists a \in A$ such that $f(a) = b$.

Question 58. What is the definition of the indicator function?

Answer.

$$1_A\colon \quad x \to \{0, 1\}$$

$$1_A = \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases}$$

Question 59. When do we say that $f : A \to B$ is inverse
Answer. If $\exists g : B \to A$ such that
$g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$.

Lecture 19

Question 60. Given $f : A \to B$, when is there a map $g : B \to A$ such that $g \circ f = \mathrm{id}_A$?
Answer. If such a g exists, using $a, a' \in A$ show f injective. Conversely show that f injective means that such a g would exist.

Question 61. Given $f : A \to B$, when is it that a map $g : B \to A$ such that $f \circ g = \mathrm{id}_B$?
Answer. We need $f(g(B)) = B$, so f must be surjective.
Conversely, if f surjective show that such a g exists.

Question 62. Show that $f : A \to B$ invertible $\iff$ f is bijective.
Answer. Consider both conditions on $f \circ g$ and $g \circ f$ and show together they imply bijectivity.

Question 63. Given $f : A \to B$, and $U \in B$, what is the pre-image of U, $f^{-1}(U)$?
Answer.

$$f^{-1}(U) = \{a \in A : f(a) \in U\}$$

Question 64. What is a relation on a set X?
Answer. A subset $R \subseteq X \times X$, usually written aRb for $(a, b) \in R$

Question 65. When is a relation R reflexive?
Answer. If $\forall x \in X$, xRx.

Question 66. When is a relation R symmetric?
Answer. If $\forall x, y \in X$, $xRy \Rightarrow yRx$.

Question 67. When is a relation R transitive?
Answer. If $\forall x, y, z \in X$, xRy and $yRz \Rightarrow xRz$.

Question 68. Given a partition of X, define the equivalence relation R where equivalence classes are precisely the parts of the partition
Answer. Define a b if a and b lie in the same part.

Question 69. Let be an equivalence relation on X. Prove the equivalence classes form a partition of X.
Answer. Verify properties of a partition.

Lecture 20

Question 70. Given an equivalence relation R in a set X, define the quotient of X by R.

Answer. $X\backslash R = \{[x] : x \in X\}$

Question 71. Prove that any subset of $\mathbb{N}$ is countable.

Answer. Apply WOP and remove element continually to produce a sequence s_n of elements for the subset. Either finite or bijection which can be constructed by considering this sequence.

Question 72. Prove that (i) X is countable
(ii) There is an injection $X \to \mathbb{N}$
are equivalent statements.

Answer. (i) $\Rightarrow$ (ii) plain.
(ii) implies bijection betwen $S = f(X)$, which is a subset of $\mathbb{N}$ so there is bijection.

Question 73. Show that (iii) $X = \emptyset$ or there is a surjection $\mathbb{N} \to X$ implies (i) X is countable.

Answer. If $X \neq \emptyset$ and there is a surjection $f : \mathbb{N} \to X$, define $g : X \to \mathbb{N}$ by $g(a) = \min f^{-1}(\{a\})$, which exists by WOP. g is injective, so X is countable.

Question 74. Prove any subests of a countable set is countable.

Answer. If $Y \subseteq X$ and X is countable, then take the injection $X \to \mathbb{N}$ restricted to Y.

Lecture 21

Question 75. Prove that $\mathbb{N} \times \mathbb{N}$ is countable by counting over diagonals.

Answer. Define $a_1 = (1, 1)$ and a_n inductively, by the sequence of coordinates that includes every point $(x, y) \in \mathbb{N} \times \mathbb{N}$ by counting through diagonals. Prove this is true by induction on $x + y$.

Question 76. Prove, algebraically, that $\mathbb{N} \times \mathbb{N}$ is countable.

Answer. Define

$$\begin{aligned} f\colon \quad & \mathbb{N} \times \mathbb{N} \to \mathbb{N} \\ & (x, y) \to 2^x 3^y \end{aligned}$$

Question 77. Prove that a countable union of countable sets is countable.

Answer. Given countable sets $A_1, A_2, A_3, \ldots$, we may list elements of A_i by

$$a_1^{(i)}, a_2^{(i)}, a_3^{(i)}, \ldots$$

Define

$$\begin{aligned} f\colon \quad & \bigcup_{n\in\mathbb{N}} A_n \to \mathbb{N} \\ & x \to 2^i 3^j \end{aligned}$$

where $x = a_j^{(i)}$ for the least i such that $x \in A_i$.
This is an injection.

Question 78. Prove that $\mathbb{R}$ are uncountable.

Answer. Cantor's diagonal argument =)

Lecture 22

Question 79. Prove there are uncountably many transcendental numbers.

Answer. If $\mathbb{R}\backslash\mathbb{A}$ were countable, then since $\mathbb{A}$ is countable, $\mathbb{R} = \mathbb{R}\backslash\mathbb{A} \cup \mathbb{A}$ would be countable. Contradiction.

Question 80. Prove for any set X, there is no bijection between X and $\mathcal{P}(X)$

Answer. Given $f : X \to \mathcal{P}(X)$,
Let $S = \{x \in X : x \notin f(x)\}$. S does not belong to the image of f
since $\forall x \in X$, S and $f(x)$ differ in the element x and thus $S \neq f(x)$, so S is not mapped to.

Question 81. Let $\{A_i i \in I\}$ be a family of open intervals of $\mathbb{R}$ which are pairwise disjoint. Prove the family is countable by considering rationals.

Answer. Each interval A_i contains a rational, and $\mathbb{Q}$ is countable, so since the intervals are disjoint we have an injection from I into $\mathbb{Q}$. Hence the family $\{A_i : i \in I\}$ is countable.

Question 82. Let $\{A_i i \in I\}$ be a family of open intervals of $\mathbb{R}$ which are pairwise disjoint. Prove the family is countable by considering length of intervals.

Answer. The set $\{i \in I : A_i \text{ has length} \leq 1\}$ is countable as it injects into $\frac{1}{2}\mathbb{Z}$.
More generally, for each $n \in \mathbb{N}$, $\{i \in I : A_i \text{ has length} \leq \frac{1}{n}\}$

Now $\{A_i : i \in I\}$ is countable as it is a countable union of countable sets.

Lecture 23

Question 83. Given non-empty sets A and B, $\exists$ injection $f : A \to B \iff \exists$ surjection $g : B \to A$.

Answer. Construct a function g which satisfies the desired condition.

Question 84. State the Schroder-Bernstein Theorem

Answer. If $f : A \to B$ and $g : B \to A$ are injections, then $\exists$ bijection $h : A \to B$.

Question 85. Prove the Schroder-Bernstein Theorem.

Answer. digest this and write it up